05-25-00

A

Scott C. Harris, Esq
PO Box 927649
San Diego CA 92192-7649
Telephone: 619-823-7778
Fax: (858) 678-5082

May 24, 2000

Attorney Docket No.: SCH/BIOMETRICS

Box Patent Application
Assistant Commissioner for Patents
Washington, DC 20231

Presented for filing is a new provisional to utility patent application of:

Applicant: SCOTT C. HARRIS

Title: USING BIOMETRICS AS AN ENCRYPTION KEY

Enclosed are the following papers, including those required to receive a filing date under 37 CFR 1.53(b):

	Pages
Specification	9
Claims	6
Abstract	1
Declaration	2
Drawing(s)	4

CERTIFICATE OF MAILING BY EXPRESS MAIL

Express Mail Label No EL584933440US

I hereby certify that this correspondence is being deposited with the United States Postal Service as Express Mail Post Office to Addressee with sufficient postage on the date indicated below and is addressed to the Assistant Commissioner for Patents, Washington, D C 20231

May 24, 2000
Date of Deposit

Janet Christy
Signature

Janet Christy
Typed or Printed Name of Person Signing Certificate

Enclosures:

— Postcard.

Under 35 USC §119(e)(1), this application claims the benefit of prior U.S. provisional application 60/160,439, filed October 19. 1999.

This case is entitled to small entity status. An executed small entity statement is attached.

A Petition to Make Special under MPEP 708.02(VIII) is attached with a separate check.

There are 25 claims, 6 independent.

Basic filing fee	$345
Total claims in excess of 20 times $9	$45
Independent claims in excess of 3 times $39	$117
Fee for multiple dependent claims	$0
Total filing fee:	$507

A check for the filing fee is enclosed. Please apply any other charges or credits to Deposit Account No. 50-1387.

If this application is found to be incomplete, or if a telephone conference would otherwise be helpful, please call the undersigned at (619) 823-7778.

Kindly acknowledge receipt of this application by returning the enclosed postcard.

Please send all correspondence to:

Customer No. 23844
SCOTT C. HARRIS
P.O. Box 927649
San Diego, CA 92192

Respectfully submitted,

Scott Harris

Scott C. Harris
Reg. No. 32,030
Enclosures
SCH/jzc

ATTORNEY DOCKET NO. SCH/BIOMETRICS

Applicant or Patentee: Scott C. Harris
Serial or Patent No.:
Filed or Issued: Herewith
For: USING BIOMETRICS AS AN ENCRYPTION KEY

VERIFIED STATEMENT (DECLARATION) CLAIMING SMALL ENTITY STATUS
(37 CFR 1.9(f) and 1.27(b)) - INDEPENDENT INVENTOR

As a below named inventor, I hereby declare that I qualify as an independent inventor as defined in 37 CFR 1.9(c) for purposes of paying reduced fees under section 41(a) and (b) of Title 35, United States Code, to the Patent and Trademark Office with regard to the invention entitled described in

[X] the specification filed herewith.
[ ] application serial no. , filed .
[ ] patent no. , issued .

I have not assigned, granted, conveyed or licensed and am under no obligation under contract or law to assign, grant, convey or license, any rights in the invention to any person who could not be classified as an independent inventor under 37 CFR 1.9(c) if that person had made the invention, or to any concern which would not qualify as a small business concern under 37 CFR 1.9(d) or a nonprofit organization under 37 CFR 1.9(e).

Each person, concern or organization to which I have assigned, granted, conveyed, or licensed or am under an obligation under contract or law to assign, grant, convey, or license any rights in the invention is listed below:

[X] no such person, concern, or organization.
[ ] persons, concerns or organizations listed below*.

*NOTE: Separate verified statements are required from each named person, concern, or organization having rights to the invention averring to their status as small entities. (37 CFR 1.27)

Full Name: ______________________________

Address: ______________________________

[X] INDIVIDUAL [ ] SMALL BUSINESS CONCERN [ ] NONPROFIT ORGANIZATION

I acknowledge the duty to file, in this application or patent, notification of any change in status resulting in loss of entitlement to small entity status when any new rule 53 application is filed or prior to paying, or at the time of paying, the earliest of the issue fee or any maintenance fee due after the date on which status as a small entity is no longer appropriate. (37 CFR 1.28(b))

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application, any patent issuing thereon, or any patent to which this verified statement is directed.

Inventor: Scott Harris

Signature: Scott Harris **Date:** 5/24/00

Attorney's Docket No.: SCH/BIOMETRICS

APPLICATION

FOR

UNITED STATES LETTERS PATENT

TITLE: USING BIOMETRICS AS AN ENCRYPTION KEY

APPLICANT: SCOTT C. HARRIS

CERTIFICATE OF MAILING BY EXPRESS MAIL

Express Mail Label No EL584933440US

I hereby certify that this correspondence is being deposited with the United States Postal Service as Express Mail Post Office to Addressee with sufficient postage on the date indicated below and is addressed to the Assistant Commissioner for Patents. Washington. D C 20231

May 24. 2000
Date of Deposit

Signature

Janet Christy
Typed or Printed Name of Person Signing Certificate

PATENT
ATTORNEY DOCKET NO. SCH/BIOMETRICS

USING BIOMETRICS AS AN ENCRYPTION KEY

Background

Biometrics allows a person to use a unique part of their body for identification purposes.

Many different body part templates have been suggested for biometrics, including fingerprints, face prints, retinal scans and DNA sequences.

Many different ways of obtaining and using biometric information are well known in the art. The body part is compared with a prestored template. A match between the part and the template allows some action to be taken. Effectively these previous biometric systems used the biometric information as a key that opens a lock. The biometric information is compared with a template. The lock opens based on the comparison.

Continuing the analogy, once the key has unlocked the lock, the user has access to information.

Encryption has also been used for security, but in a different way. Encryption is used to change the information itself. No lock and key is necessary - the information can be disseminated, and the decryption key can be used to retrieve it.

Encryption is often used for messages, e.g. by email. Encryption is also used to keep private certain information in an account, for example.

One popular kind of encryption is public key cryptography. The encryption key is public and anyone can use it. Only the person having the private key can decrypt a message, however. If user A encrypts a message with user B's public key, only B can decrypt the message. No one else, not even user A, can decrypt the message. Other similar cryptosystems are known. All have in common that there must be a decryption key -£ typically a large number.

Summary

It can be difficult to store the key for an encryption system. For instance, in a public key cryptography system, the user typically stores their private key inside their computer. However, a person with access to the user□s computer can obtain access to the private key with much less security than is provided by the key itself. The private key is too long to memorize (e.g. 128 bits), and instead must be transported for example on a transportable storage medium. This is by itself inconvenient.

The present application teaches a way of using biometrics to form an encryption and/or decryption key. The biometric information itself is translated into an encryption and/or decryption key. Therefore, the key is always available to the user, since it is formed based on the user□s body parts.

The key is formed by comparing the relationship of parts of the biometric information.

An aspect of the invention uses a sequence of biometric information as the key. Only the specified sequence forms a proper key. Therefore, surreptitiously obtaining the user's biometric information will not enable forming a proper key without also knowing the proper combination.

Another aspect uses relative information from the biometric information to form the key. In this way, the key is formed independent of the absolute dimensions of the biometric information. The key that is formed can use the obtained information as a "seed", or can use the information directly.

Yet another aspect uses the concept of relative dimensions with biometrics as they have been conventionally been conceived, to determine if the biometric information fits a proper profile, and use that recognition to allow access.

Brief Description of the Drawings

These and other aspects of the invention will be described in detail with reference to the accompanying drawings, wherein:

Figure 1 shows an embodiment;

Figure 2 shows a layout of an exemplary fingerprint;

Figure 3 shows a flowchart of operation; and

Figure 4 shows a special kind of fingerprint reader, and an example of its operation.

Description of the Embodiments

An embodiment is shown in Figure 1. A personal computer system 99 includes a biometric reading device 102. The personal computer 99 itself runs an application software layer 110 (e.g. an operating system) that includes security software 120. The security software relies on a cryptographic key for its proper operation.

In a particularly preferred embodiment, the security software 120 is a public key encryption/decryption system. The private key is based on the user□s biometric information.

Figure 1 shows the user placing a body part 100 into a biometric reading device 102. The information from the user□s body part 100 is transmitted along line 105 to software layer

110, running the application program 120, for example, a security program.

The biometric device 102 can be any conventional fingerprint reader, which reads and produces an analog image or digital sample of the fingerprint. Either case produces what is effectively an image of the user□s fingerprint. The image is conceptually shown in Figure 2. All fingerprints have certain general characteristics. The fingerprints have a number of ridges 222, 224, 226, which come together at a substantially center point 200. The center point of the user's fingerprint is taken as a center line. A number of ridges are formed around that center point. The lines on each user□s fingerprint are different. A typical fingerprint may have approximately 25 to 35 lines in the width wise direction, and approximately 30 to 60 lines in the length wise direction. In this embodiment, the center point 200 is used as a point to draw reference lines. The reference line 210 defines a widthwise direction and the line 220 defines a lengthwise direction.

Since a typical fingerprint scanner provides an image of the entire fingerprint, all of this processing can be done in the computer 99. This is carried out according to the flowchart of Figure 3 which may run on computer 110.

At 300, the system finds a reference point and defines reference lines. The reference lines can include one line such as 210 in Figure 2, or alternatively can be more than one reference line. A second reference line, for example could be reference line 220 in Figure 2. Since the whole image of the fingerprint is available these lines can easily be made parallel or perpendicular to an "axis".

At 302, the system determines ridge spacing along the reference line. For example, in Figure 2, a first ridge 222 closest to the determined center is taken as the first found ridge. This is the ridge closest to the reference point, and avoids determination of the edge of the fingerprint, or determining what is the first ridge. The ridge 222 in this embodiment is defined as the ridge, on the left, closest to the center. The second ridge 224 is the next ridge over to the left. The ridge 226 after that is the next ridge to the left. For purposes of illustration, the system determines the spacing between 10 ridges on the left and 10 ridges on the right. This produces 20 values.

At 304, the system finds the average of all the values.

Then at 306 the current value is compared to the average. "0" is defined if the current value is higher than the average, or a “1" if the current value is lower than the average. If the spacing is equal to the average, then the value is taken as the inverse of the bit before it.

A simple example is shown in Figure 4. The sensor 100 detects distances, here shown as 5, 4, 6, 8, 9 and 4. The total of these is 36, and since third are six distances, the average is 6. Now each of the values is compared with the average, to obtain 00X110, since the last bit represents a tie. This flips the x bit before it to obtain 001110. At 308, the value thus obtained is stored as part n of the key. 310 detects if the key is complete. If so, the key is used at 312. If not, flow returns to 300 to obtain another part of the key. This can use another specified reference line, e.g., a perpendicular line such as shown as line 220. It could alternately and more preferably be biometric information from a different biometric part, e.g. a different finger.

The lines that are used to obtain the information can also be at specified angles to the reference lines, e.g., at 22 degrees. The angles can be set, or can be entered by the user, as a form of personal identification. For example, the user can enter 22 while a specified finger is in the reader. This takes the line along 22 degrees. It effectively forms a PIN that must be entered to obtain the proper code from the biometric information.

By piecing together the decryption key from different body parts, the present system also provides an additional layer of security. The system above has described getting about 20 digits from a single biometric scan. This may correspond to 20 bits. If two orthogonal dimensions are defined as shown in the picture, this doubles the amount of information to 40 bits. However, by combining three fingerprints, a much more robust key length of 120 bits can be obtained. Moreover, additional security is provided by the specific selection of fingerprints. Only the user knows which biometric items to input, how many, and in which order. This effectively forms a barrier against others using this information.

An advantage of the present system comes from the use of relative, rather than absolute, information. No calibration is necessary, since each of the values is calculated based on comparing parts of the fingerprint to itself, not to some absolute reference. The digits are unambiguous, since there is no calibration, only an internal sensing of relationships among the different parts. The only necessary commonality is resolution -- the image sensor used must have sufficient resolution to sense each ridge of the fingerprint.

Figure 4 shows an embodiment in which the fingerprint sensor is actually an image sensor chip, e.g., a CCD image sensor or active pixel sensor type device or infra-red photodetect. The chip□s active surface is usually placed to receive the image of a larger area. However, in this embodiment, the pixels of the sensor are directly mapped to the user□s finger. The finger is placed directly on the sensor. The position and orientation of the user□s finger does not matter, since an unambiguous reference is obtained from the comparison of the different parts of the biometric information.

Another embodiment uses the relative relationship of the biometric information as described above in the conventional way that biometric information has been used. The relative relationship among the biometric information is used to form a number. That number is compared against a prestored number to determine identity. The test yields a pass if the information agrees.

Other biometric information can be used in a similar way. Retinal scans can be used by determining the same kind of relationship among lines of the scan, for example.

Other embodiments are within the disclosed invention.

What is claimed is:

1. A method, comprising:

obtaining information about a biometric part of a user's body; and

forming a cryptographic key based on said biometric information without determining absolute dimensions of said biometric information.

2. A method as in claim 1 wherein said forming comprises determining ratios between different portions of said biometric information.

3. A method as in claim 1 further comprising entering a plurality of different biometric features in a sequence, an order of the sequence forming the code.

4. A method as in claim 1 further comprising entering information that is supplemental to the biometric information, the supplemental information indicating parts of the biometric information which should be used to form the code.

5. A method as in claim 1, wherein said biometric part is a fingerprint.

6. A method as in claim 4 wherein the supplemental information includes an angle of a line used to obtain the information.

7. A method comprising:

entering biometric information;

determining relationships between different parts of the biometric information; and

using said relationships to form a cryptographic key.

8. A method as in claim 7 further comprising using said cryptographic key to encrypt or decrypt information.

9. A method as in claim 8 wherein said relationship includes a ratio between different parts of an image.

10. A method as in claim 8 wherein said biometric information comprises a sequence of different items of biometric

information which are pieced together to form a code that is dependent both on the pieces of the biometric information and on the sequence.

11. An apparatus, comprising:

a biometric information obtaining part;

a computer;

wherein said computer is responsive to obtain an image from the biometric information part, extract values from the biometric information part, and use said values to encrypt or decrypt a message.

12. An apparatus as in claim 11 wherein said computer obtains a plurality of different biometric information parts, and wherein both the content of the information parts and a sequence of entry of the information parts, forms the code.

13. An apparatus as in claim 12 wherein the information is formed by relationships between different parts of an image of the biometric information.

14. A fingerprint sensor, comprising:

an image sensor chip forming a plurality of pixels for sensing an image, said chip having an active surface which receives said image, said active surface adapted to receive a finger thereon to obtain a fingerprint therefrom and produce an output indicative of the fingerprint.

15. A sensor as in claim 14 further comprising a computer part, connected to said image sensor, receiving said output, and using said output to form a cryptographic key.

16. A method as in claim 15 wherein said cryptographic key is formed from a relationship between different parts of the image.

17. A method, comprising:

obtaining information about a plurality of biometric parts of a user's body;

forming a cryptographic key based on said information using both the plurality of parts and a sequence of entry of the plurality of parts; and

using said cryptographic key to one of encrypt or decrypt a message.

18. A method as in claim 17 wherein said forming comprises determining ratios between different portions of said biometric information.

19. A method as in claim 17 further comprising entering information that is supplemental to the biometric information, the supplemental information indicating parts of the biometric information which should be used to form the code.

20. A method as in claim 17, wherein said biometric part is a fingerprint.

21. A method as in claim 19 wherein the supplemental information includes an angle of a line used to obtain the information.

22. A method, comprising:

obtaining information about a biometric part of a user's body;

obtaining additional information; and

forming a cryptographic key based on both said biometric information and said additional information.

23. A method as in claim 22 wherein said forming comprises determining ratios between different portions of said biometric information.

24. A method as in claim 22 further comprising entering a plurality of different biometric features in a sequence, an order of the sequence forming the code.

25. A method as in claim 22 wherein the supplemental information includes an angle of a line used to obtain the information.

Abstract

An image of an biometric part is used as encryption or decryption key. The biometric part image is obtained, and items within the biometric part are analyzed. Relationships between those parts are determined, e.g. ratios between different parameters of different parts. Those ratios are then used to form the key. A sequence of biometric information can used in which case both the information itself and the sequence are used to form to the key.

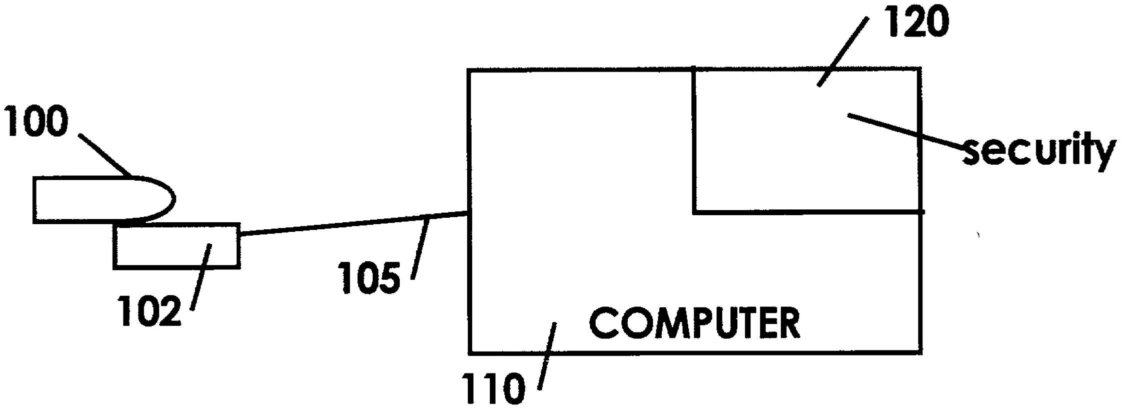

FIGURE 1

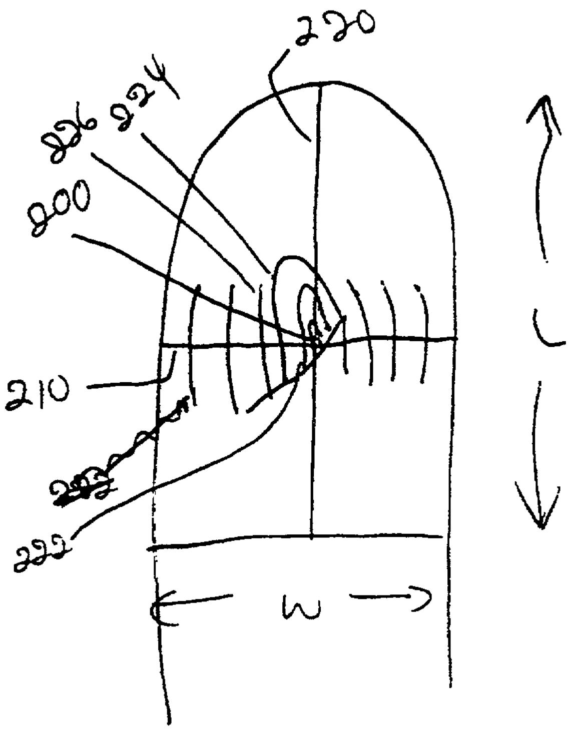

FIG 2

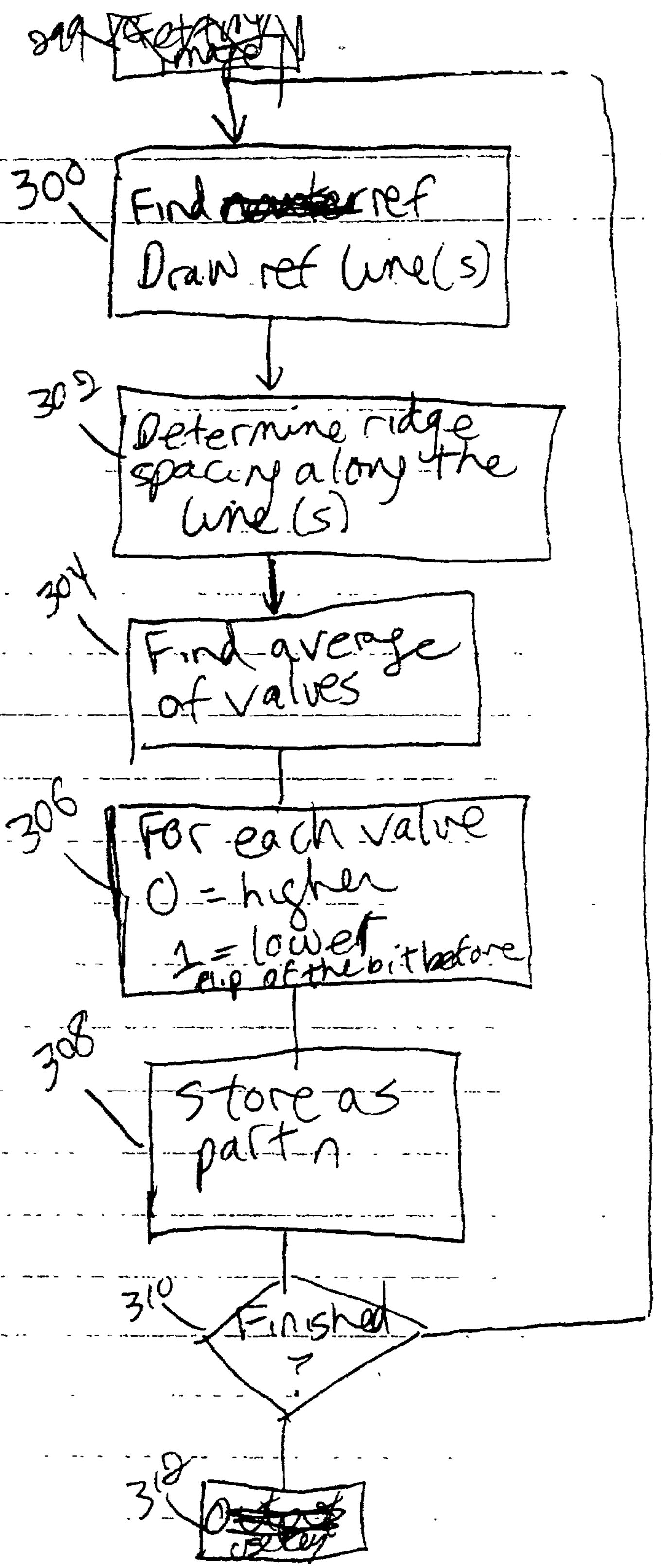
299
Get any image
300
Find ~~master~~ ref
Draw ref line(s)
302
Determine ridge spacing along the line(s)
304
Find average of values
306
For each value
0 = higher
1 = lower
flip of the bit before
308
Store as part n
310
Finished ?
318
~~Output~~
Key

FIG 3

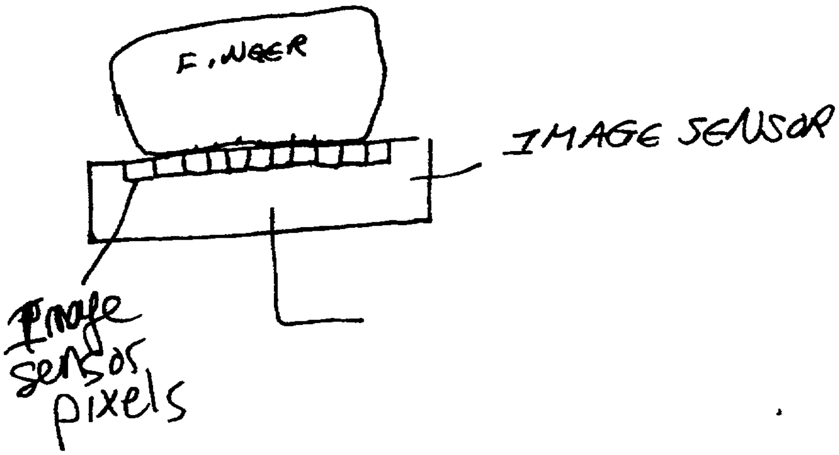

FIG 4

Attorney's Docket No.: SCH/BIOMETRICS

COMBINED DECLARATION AND POWER OF ATTORNEY

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled USING BIOMETRICS AS AN ENCRYPTION KEY, the specification of which:

[x] is attached hereto.
[] was filed on ________ as Application Serial No. ___________ and was amended on ______________.
[] was described and claimed in PCT International Application No. ______________ filed on ______________ and as amended under PCT Article 19 on ______________.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose all information I know to be material to patentability in accordance with Title 37, Code of Federal Regulations, §1.56.

I hereby claim the benefit under Title 35, United States Code, §119(e)(1) of any United States provisional application(s) listed below:

U.S. Serial No.	Filing Date	Status
60/160.439	October 19, 1999	Pending

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowledge the duty to disclose all information I know to be material to patentability as defined in Title 37, Code of Federal Regulations, §1.56(a) which became available between the filing date of the prior application and the national or PCT international filing date of this application:

U.S. Serial No.	Filing Date	Status

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate or of any PCT international application(s) designating at least one country other than the United States of America listed below and have also identified below any foreign application for patent or inventor's certificate or any PCT international application(s) designating at least one country other than the United States of America filed by me on the same subject matter having a filing date before that of the application(s) of which priority is claimed:

Country	Application No.	Filing Date	Priority Claimed
			[] Yes [] No
			[] Yes [] No

Combined Declaration and Power of Attorney

Page 2 of 2 Pages

Address all telephone calls to SCOTT C. HARRIS at telephone number (619) 823-7778.

Address all correspondence to SCOTT C. HARRIS at:

Customer No. 23844
Scott C. Harris
P.O. Box 927649
San Diego, CA 92192-7649

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patents issued thereon.

Full Name of Inventor: Scott C. Harris

Inventor's Signature: Scott C Harris Date: 5/24/00

Residence Address: 3329 Cerros Redondos, Rancho SantaFe, CA 92067

Citizenship: USA

Post Office Address: P.O. Box 927649, San Diego, CA 92192